RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAB2-M05

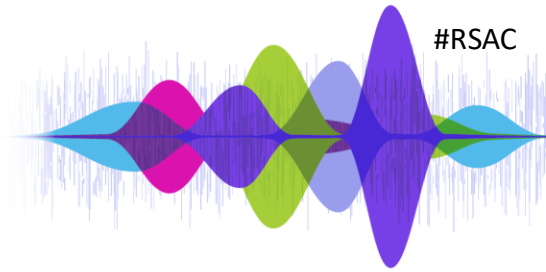
Deepfake Cyber Extortion: A Tabletop Learning Lab

Sherri Davidoff

Founder
LMG Security
https://www.linkedin.com/in/sherri-davidoff/

Matt Durrin

Director of Training and Research
LMG Security
https://www.linkedin.com/in/evilmatt



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

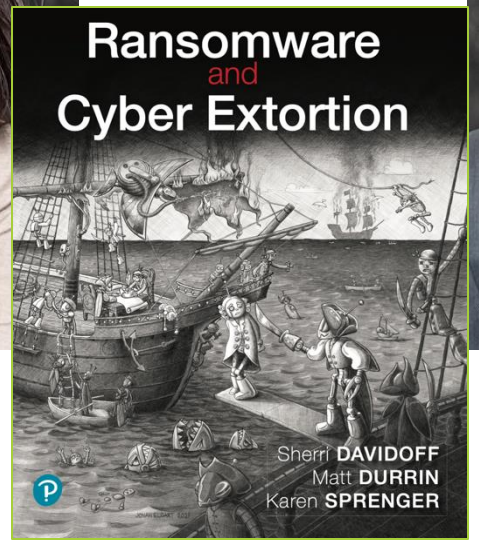
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Who Are We?

Sherri Davidoff

Founder & CEO

MIT EE/CS, GCFA, GPEN



Our Book!

Matt Durrin

Director of Training & Research

Evil, sometimes.

LMG SECURITY

Penetration Testing

Advisory & Compliance

vCISO & Support

Cybersecurity Training

Today's Tabletop Exercise

- Deep Fake & Cyber Extortion
  - Threat actors leverage deep fakes
  - Cyber extortion & attempted fraud
- Consider customer-facing impacts
- Practice/evaluate communication
  - Internal & external
- Talk through response strategies
- Interactive breakout exercises
- Lots of discussion!

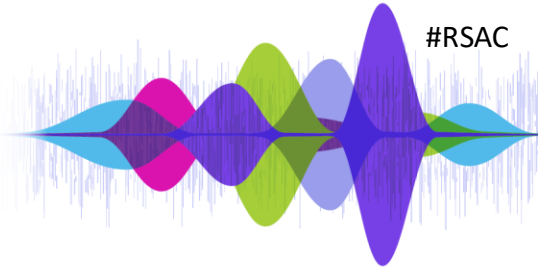
Maximizing Value of the Exercise

- Participate! Speak up & ask questions
- There are NO perfect responses
- There are NO dumb questions
- Not an audit or “gotcha” exercise
- Have fun!

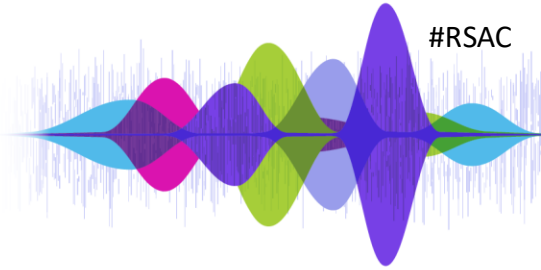
Phase 1: Deepfake Video Crisis

- A video of HackMe Inc.’s CEO appears on YouTube and social media, causing public embarrassment.
- Marketing is locked out of social media accounts!

Phase 1: Small Group Discussion



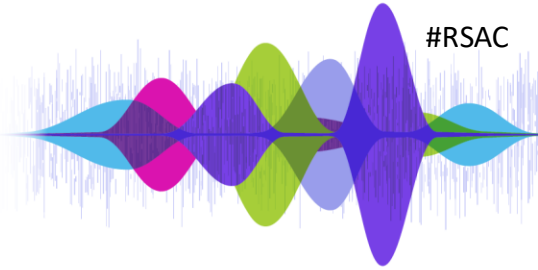
- How do you authenticate the deepfake video?
- What are your first 3 steps in responding to the crisis?
- How do you coordinate with PR, legal, and social media platforms?
- What internal communications do you send to employees and executives?



Phase 1: Large Group Debrief

- Let’s share top response actions!
- Key strategies: digital forensics, crisis PR, access recovery steps.

Response Tips

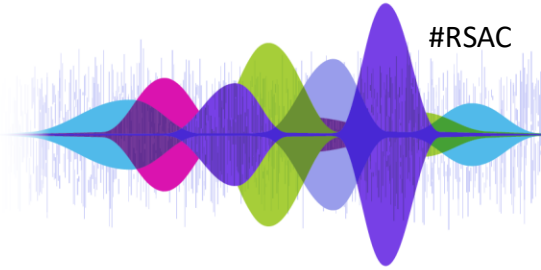


- Verify authenticity using deepfake detection tools, metadata analysis, and forensic techniques.
- Contact your cyber insurer immediately, if applicable.
- Respond quickly with a clear communication plan, acknowledging the issue without amplifying it.
- Engage PR and legal teams to craft messaging for media, employees, and stakeholders.
- Work with platform providers (YouTube, Twitter, etc.) to request takedowns if necessary.

Phase 2: Ransom Demand & Voice Deepfake

- The CEO receives a phone call from a number matching her own, with her voice on the line, representing a ransomware gang. The gang demands $6MM to stop releasing more deepfake videos and return control of the company's social media.

Phase 2: Small Group Discussion



- Do you engage with the attacker? Why or why not?
- What's your ransomware/extortion policy?
- Should law enforcement, cyber insurers, or regulatory agencies be involved?
- How do you respond to employees, clients, and stakeholders?

Phase 2: Large Group Debrief

- Present your decisions on ransom demands and stakeholder communication.
- Let’s discuss legal, ethical, and operational considerations.

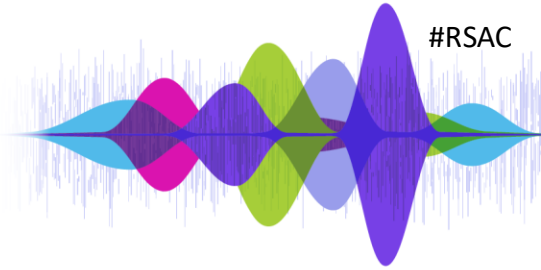
Response Tips

- Consult with your cyber insurer before paying, if applicable
- Evaluate whether paying aligns with legal, ethical, and insurance considerations.
- Use out-of-band verification before responding to the attacker.
- Strengthen MFA and social media recovery processes to prevent further extortion.

Phase 3: Executive Impersonation via Teams

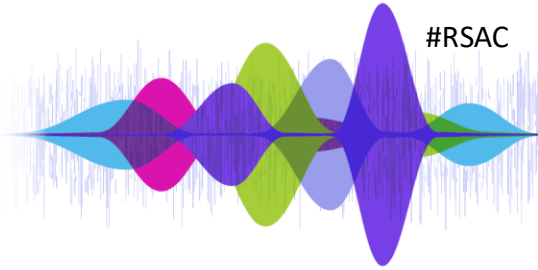
- Hackers use deepfake video and voice cloning to infiltrate Teams calls, posing as executives and spreading confusion. They claim to have accessed sensitive emails and chats.

Phase 3: Small Group Discussion

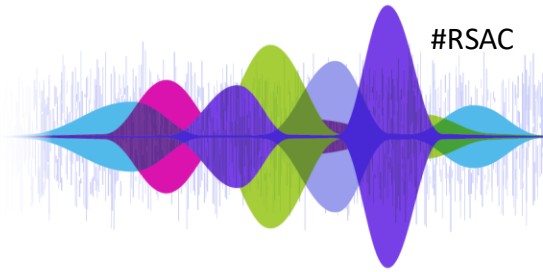


- How do you verify executive communications (calls, emails, video meetings)?
- What authentication measures should be implemented immediately?
- How do you prevent internal confusion and misinformation?

Phase 3: Large Group Debrief



- Teams present verification strategies and security updates.
- Let’s talk about real-world deepfake detection technologies and best practices.



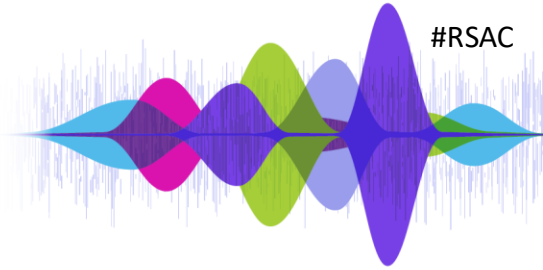
Response Tips

- Update Teams configuration to restrict attendance.
- Implement mandatory video authentication (e.g., real-time liveness detection).
- Require secondary identity verification (e.g., a call-back or challenge-response questions).
- Use internal awareness training to educate employees about deepfake threats.
- Monitor for unusual login behaviors, such as logins from unexpected locations.

Phase 4: CFO Deepfake & Financial Fraud Attempt

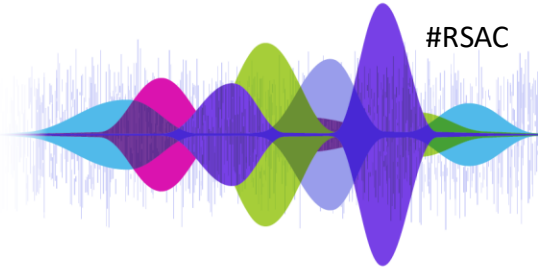
- The Finance Director receives a video call from the CFO instructing a $6MM wire transfer. Suspicious, the Finance Director calls the real CFO via a different channel and confirms the request was fake.

Phase 4: Small Group Discussion

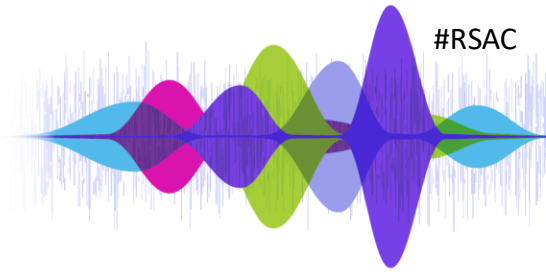


- How do you verify executive communications (calls, emails, video meetings)?
- What authentication measures should be implemented immediately?
- How should finance teams verify high-risk transactions?
- What policies and training should be introduced post-incident?

Phase 4: Large Group Debrief

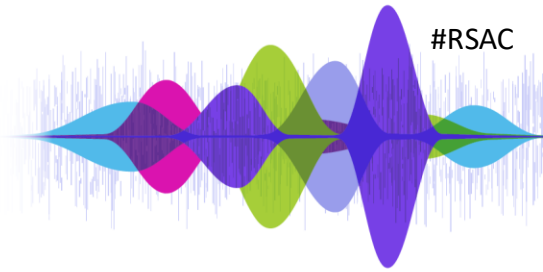


- Teams present verification strategies and security updates.
- Let’s talk about real-world deepfake detection technologies and best practices.



Response Tips

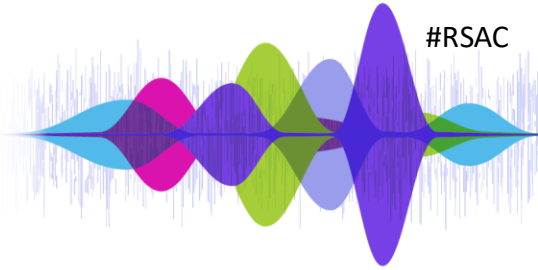
- Require multi-person approval for high-value transactions.
- Train finance teams to recognize deepfake fraud indicators.
- Use AI-driven fraud detection tools to flag unusual requests.
- Implement strict verification policies such as call-backs on a known, pre-verified number.



Time to Brief Your Board!

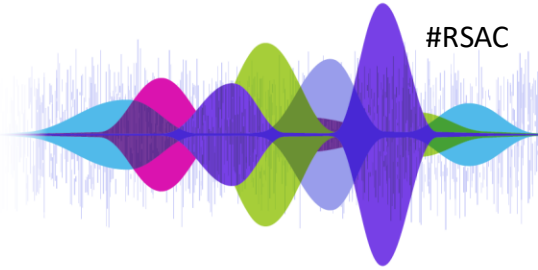
- Each team delivers a 2-minute board-level briefing
- How well did your organization respond?
- What policies need to change immediately?
- What will you present to executive leadership about deepfake threats?

Wrap-Up & Board-Level Briefing



- Review response effectiveness and lessons learned.
- What did you learn today?
- Final reflections and Q&A.

Apply What You Have Learned Today



Next week you should:

- Identify critical assets vulnerable to deepfake cyber extortion.

In the first three months following this presentation you should:

- Assess who has access to critical systems and communication channels.
- Define authentication controls to prevent deepfake-related fraud.

Within six months you should:

- Implement security systems for deepfake detection and verification.
- Establish robust policies to mitigate AI-driven social engineering threats.

Questions?

- Matt Durrin & Sherri Davidoff
- info@LMGsecurity.com
- @LMGSecurity

RSAC 2025 Conference

Many Voices.
One Community.

For more information:

Sherri Davidoff / Matt Durrin

info@LMGsecurity.com